

REMARKS

Claims 12, 14-16 and 18-33 are pending in the present application. In the above amendments, claims 12, 14-16 and 18-22 have been amended, and new claims 23-33 have been added.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 103

The Examiner rejected claims 12, 14-16 and 18-22 as being allegedly unpatentable over Dierks et al., The TLS Protocol, Version 1.0 (the Dierks publication) in view of U.S. Patent No. 7,237,261 to Huber et al. (the Huber patent).

The rejection of claim 12 as being unpatentable over the Dierks publication in view of the Huber patent, is respectfully traversed. Claim 12, as amended, recites a “method for fast generation of a cryptographic key, comprising: generating a first public key for encrypting a first wireless communication; and generating, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in the second wireless communication, wherein the second public key is independent of the first public key.” Support for the amendment to claim 12 is in the specification in paragraphs [0020] through [0024], and in Figure 2, steps 204-208. The Dierks publication discloses that the “cryptographic parameters of the session state are produced by the TLS Handshake Protocol When the TLS client and server first start communicating, they agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use public-key encryption techniques to generate shared secrets.” See, page 28, section 7.3, “Handshake Protocol overview”, first paragraph. Applicants respectfully assert that these steps disclosed by the Dierks publication necessarily take place after initiation of the communication between the TLS client and the server. Thus, the Dierks publication fails to disclose or suggest, “generating, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in the second wireless communication, wherein the second public key is independent of the first public key,” as recited in claim 12. Further, the Huber patent fails to remedy the disclosure deficiencies of the Dierks publication. Therefore,

since the Dierks publication and the Huber patent do not disclose or suggest all of the recited features, Applicants respectfully request the Examiner to withdraw the rejection of claim 12.

It is respectfully submitted that dependent claims 14-15 and 32 are at least allowable for the reasons given above in relation to independent claim 12.

Claims 16-31 and 33 are wireless communication device, processor, and computer program product claims having features defined by language similar to that of method claims 12, 14-15 and 32. It is respectfully submitted that claims 16-31 and 33 are at least allowable for the reasons given above in relation to claims 12, 14-15 and 32.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **January 25, 2008**

**By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295**

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502